(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－93242

(43)公開日　平成９年(1997)４月４日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ			技術表示箇所
Ｈ０４Ｌ	9/14			Ｈ０４Ｌ	9/00	６４１	
	9/16			Ｈ０４Ｎ	1/44		
Ｈ０４Ｎ	1/44			Ｈ０４Ｌ	9/00	６４３	

審査請求　未請求　請求項の数６　ＯＬ　（全４頁）

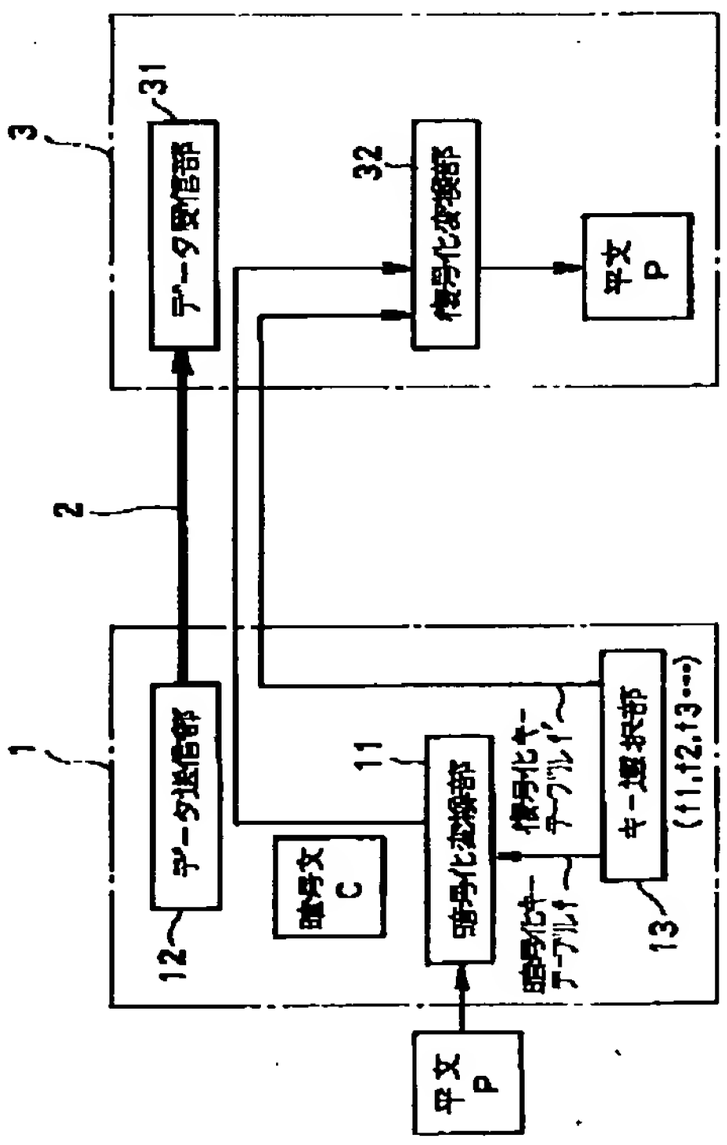
(21)出願番号　特願平7－249593

(22)出願日　平成７年(1995)９月27日

(71)出願人　000232047
日本電気エンジニアリング株式会社
東京都港区芝浦三丁目18番21号
(72)発明者　武島　一彰
東京都港区芝浦三丁目18番21号　日本電気エンジニアリング株式会社内
(74)代理人　弁理士　京本　直樹　（外２名）

(54)【発明の名称】　データ送受信装置

(57)【要約】
【課題】　暗号文を電話回線等にて送信するとき、盗聴による機密保持をより強固にする。
【解決手段】　送信側１において、平文Ｐを暗号化変換部１１にて暗号文Ｃに変換するとき、キー選択部１３においてジョブ単位に暗号化キーテーブルをランダムに変化させて暗号化する。
【効果】　ジョブ単位に暗号化キーテーブルを任意に変えるようにしているので、長期間同一の回線の暗号データを盗聴されても、暗号化方法を解析することは困難になる。



【特許請求の範囲】

【請求項１】　ジョブ単位でデータの送信を行うデータ送信装置であって、ジョブ毎に互いに異なる暗号化キーテーブルを選択する暗号化キー選択手段と、この選択された暗号化キーテーブルに従って送信データの暗号化を行う暗号化手段と、前記暗号化キーテーブルを特定するための情報を生成する特定情報生成手段とを含み、前記暗号化手段による暗号化出力と前記特定情報生成手段の特定情報とを送信するようにしたことを特徴とするデータ送信システム。

【請求項２】　前記特定情報は、前記暗号化キーテーブルに対応する復号化キーテーブルの内容であることを特徴とする請求項１記載のデータ送信装置。

【請求項３】　前記特定情報は、前記暗号化キーテーブルの各々に対して固有に割当てられた識別番号であることを特徴とする請求項１記載のデータ送信装置。

【請求項４】　請求項１記載のデータ送信装置からのデータを受信するデータ受信装置であって、前記特定情報に対応する復号化キーテーブルに従って受信暗号化データを復号化する復号化手段を含むことを特徴とするデータ受信装置。

【請求項５】　請求項２記載のデータ送信装置からのデータを受信するデータ受信装置であって、前記復号化キーテーブルの内容に従って受信暗号化データを復号化する復号化手段を含むことを特徴とするデータ受信装置。

【請求項６】　請求項３記載のデータ受信装置であって、前記識別番号に対応する復号化キーテーブルの内容に従って受信暗号化データを復号化する復号化手段を含むことを特徴とするデータ受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデータ送受信装置に関し、特にデータ通信の機密保持のために送信データを暗号化して送出するようにしたデータ送受信装置に関するものである。

【０００２】

【従来の技術】電話回線等を用いてデータ通信を行う場合には、機密保持のためにデータの内容を第三者が判読できない様にする必要がある。そこで、送信側で送受データを暗号化して送出し、受信側で復号化する技術がある。

【０００３】図５はこの種の暗号化／復号化装置の一例を示すものである。図５を参照すると、送信側１においては、送出すべきデータである平文Ｐを暗号化変換部１１にて暗号化キーテーブルｆを用いて暗号文Ｃを生成し、データ送信部１２から電話回線等の通信網２を介して送信する。

【０００４】受信側３では、データ受信部３２にて復号化キーテーブルｆ´を用いて復号化し、平文Ｐを得るようになっている。尚、復号化キーテーブルｆ´は暗号化

キーテーブルｆの逆変換テーブルを意味する。

【０００５】特開平５－１１５０１３号公報には、ファクシミリ通信において、暗号化用のキーテーブルを決定するために、全装置が共通に有する複数のキーテーブルの中から使用するキーテーブルを通信するファクシミリ装置の組合せにより自動的に決定する方法が開示されている。

【０００６】

【発明が解決しようとする課題】図５に示す従来の暗号化／復号化装置においては、送信側１の内部に記憶されている固定の暗号化キーテーブルｆを用いているために、長時間同一の回線の暗号データを不正に盗聴されることで、暗号化方法を解析されてしまい、データの機密性が失われるという問題がある。

【０００７】特開平５－１１５０１３号公報においては、通信毎に通信するファクシミリ装置の組合せにより暗号化キーテーブルを決定するものであり、送信側及び受信側双方の電話番号やパスワード等の情報を基に、使用する暗号化キーテーブルを演算して決定するようになっているので、演算処理が必要であり、演算処理のためのハードウェアやソフトウェアも必要になり、小型化，低コスト化が図れないという問題もある。

【０００８】本発明の目的は、極めて簡単な構成でデータの機密保持をより高める様にしたデータ送受信装置を提供することである。

【０００９】

【課題を解決するための手段】本発明によれば、ジョブ単位でデータの送信を行うデータ送信装置であって、ジョブ毎に互いに異なる暗号化キーテーブルを選択する暗号化キー選択手段と、この選択された暗号化キーテーブルに従って送信データの暗号化を行う暗号化手段と、前記暗号化キーテーブルを特定するための情報を生成する特定情報生成手段とを含み、前記暗号化手段による暗号化出力と前記特定情報生成手段の特定情報とを送信するようにしたことを特徴とするデータ送信システムが得られる。

【００１０】また、本発明によれば、上記データ送信装置からのデータを受信する受信装置であって、前記復号化キーテーブルの内容に従って受信暗号化データを復号化する復号化手段を含むことを特徴とするデータ受信装置が得られる。

【００１１】

【発明の実施の形態】本発明の作用について述べる。送信側において、ジョブ毎に暗号化キーテーブルを変化して送出するが、同時にこの暗号化キーテーブルを特定する情報をも送出する。こうすることにより、暗号化キーテーブルがジョブ毎にその都度変化するので、データ機密性はより一層向上可能となる。

【００１２】以下に図面を用いて本発明の実施例について説明する。

【００１３】図１は本発明の一実施例のシステムブロック図であり、図５と同等部分は同一符号により示されている。本実施例の送信側１においては、キー選択部１３が設けられており、このキー選択部１３において、ジョブ毎の送信データ（平文Ｐ）についての暗号化キーテーブルを任意（ランダム）に選択し、暗号化変換部１１にてこの選択された暗号化キーテーブルを用いて平文Ｐの暗号化を行うものである。

【００１４】受信側３において、復号化する際に暗号化キーテーブルが特定されなければ、復号化はできないので、送信側１のキー選択部１３において、選択した暗号化キーテーブルｆの逆変換用の復号化キーテーブルｆ´を復号化用情報として送信するようになっている。

【００１５】従って、受信側３においては、この復号化キーテーブルｆ´を用いて復号化変換部３２で受信データの復号化が行われ、平文Ｐが得られることになる。

【００１６】図２は暗号化キーテーブルの一つの例を示しており、図３はこの図２に示した暗号化キーテーブルに対応する逆変換用の復号化キーテーブルを示している。これ等キーテーブルについて簡単に説明すると、情報処理ではデータをバイト単位の数値（０～２５５）として処理しており、よって文章つまり文字の並びをデータ送信するには、連続したバイトデータの並びとして表現する必要がある。例えば一英文字の場合一国際共通であるＡＳＣＩＩコード系が使用されるが、このＡＳＣＩＩコードでは、１バイト（０～２５５）に英文字１文字を夫々割当てている。

【００１７】図２の「入力」は送信すべき入力文字の１バイト単位の数値であり、「出力」は暗号化の際の変換数値を示している。

【００１８】また、図３は図２の暗号化キーテーブルに対応する逆変換用復号化キーテーブルの内容であり、図２の「入力」と「出力」とが逆になっていることが判る。

【００１９】この様な暗号化キーテーブルの種類は２５６！とおり存在するので、キー選択部１３ではこの２５６！とおりのキーテーブルからジョブ毎に任意にランダムに選択するようになっている。このランダムな選択は乱数表等を用いて容易に実現可能である。

【００２０】図１の実施例においては、ジョブ毎の送信データに関して暗号化キーテーブルを変換する様にして機密保持を行っているが、暗号化データと共に復号化キーテーブルも同時に送信しているために、機密保持の完全さは担保できない。

【００２１】そこで、図４に示す如き第２の実施例が得

られる。図４において図１と同等部分は同一符号により示している。本実施例では、２５６！種類の暗号化キーテーブルの各々に対してそれを特定するためのＩＤ（識別）番号を予め付与しておき、キー選択部１３にてランダムに選択された暗号化キーテーブルの各ＩＤをキー番号生成部１４にて生成し、暗号化キーテーブルを送る代りに、これらＩＤ情報のみを暗号文Ｃと共に送るようにしている。

【００２２】従って、受信側３では、このＩＤ情報により復号化キーテーブルを復号化キー選択部３３にて選択して、受信暗号文Ｃを復号して平文Ｐへ戻すようにするのである。

【００２３】こうすることにより、暗号キーテーブルを他に知られることは全くなくなり、極めて機密性の高い通信システムとなるものである。

【００２４】

【発明の効果】叙上の如く、本発明によれば、ジョブ毎に暗号化キーテーブルの内容が変更されるので、長期間同一の回線の暗号データを不正に盗聴されたとしても、暗号方法の解析が困難であり、また暗号化キーテーブルの内容を送出する代りに、暗号化キーテーブルのＩＤ情報のみを送出することにより、尚一層の機密性の向上が図れるという効果がある。

【図面の簡単な説明】

【図１】本発明の一実施例のブロック図である。

【図２】暗号化キーテーブルの内容の一例を示す図である。

【図３】図２の暗号化キーテーブルに対応する逆変換のための復号化キーテーブルの内容の一例を示す図である。

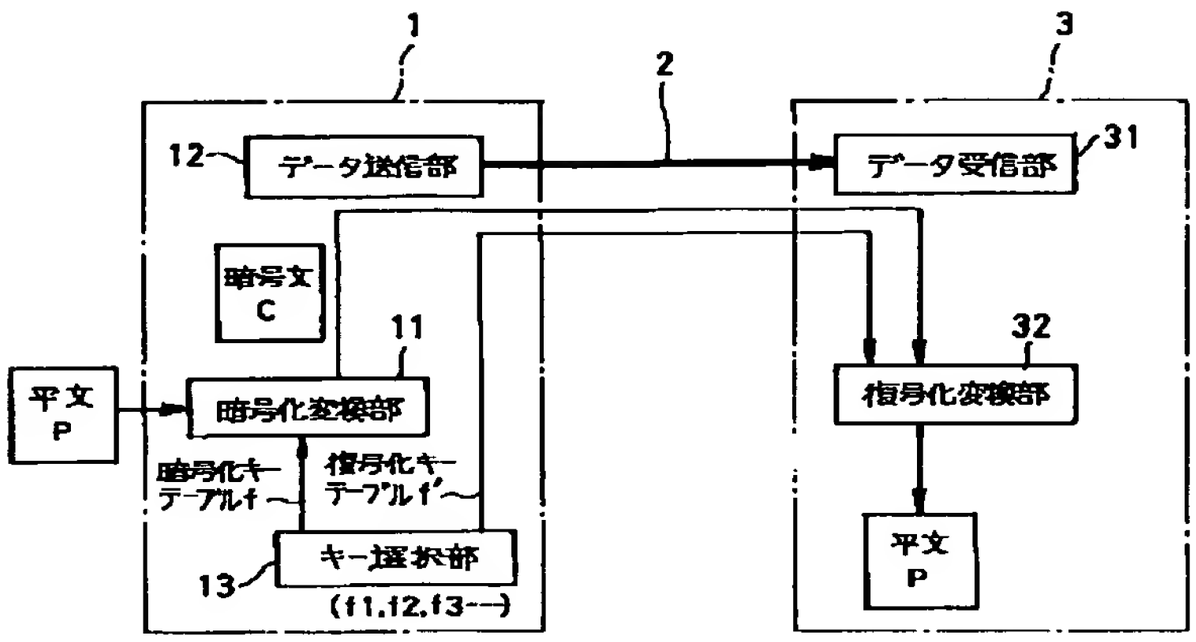
【図４】本発明の他の実施例のブロック図である。

【図５】従来の暗号／復号化機能を有する送受信装置のブロック図である。

【符号の説明】

１　送信側
２　回線
３　受信側
１１　暗号化変換部
１２　データ送信部
１３　キー選択部
１４　キー番号生成部
３１　データ受信部
３２　復号化変換部
３３　復号化キー選択部

【図1】



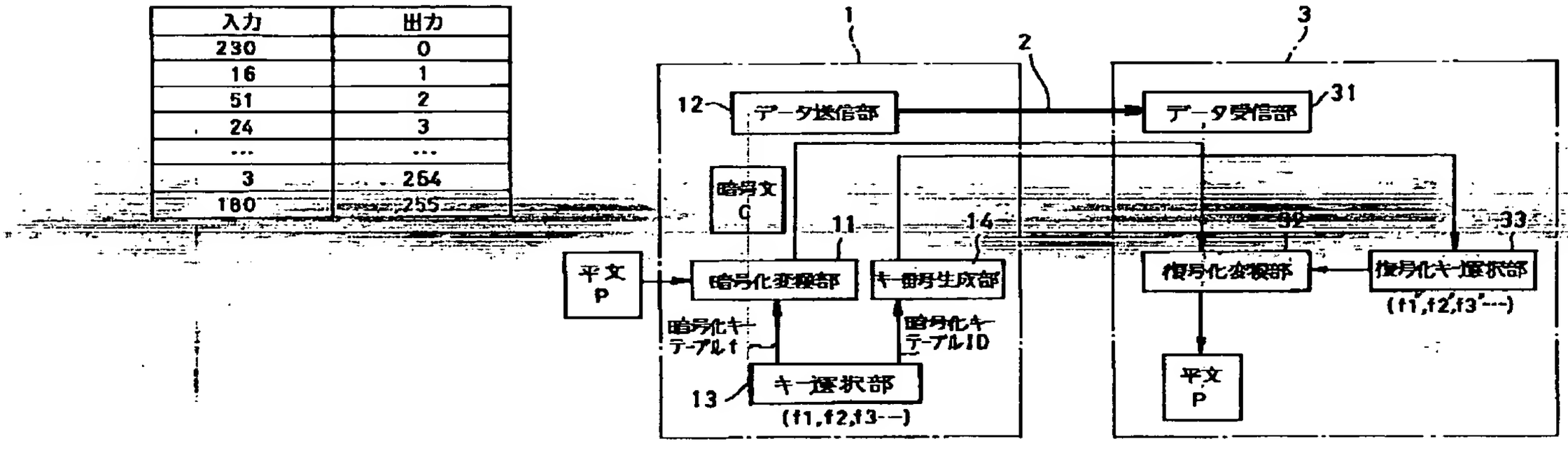
【図2】

入力	出力
0	230
1	16
2	51
3	24
…	…
254	3
255	180

【図3】

入力	出力
230	0
16	1
51	2
24	3
…	…
3	254
180	255

【図4】



【図5】